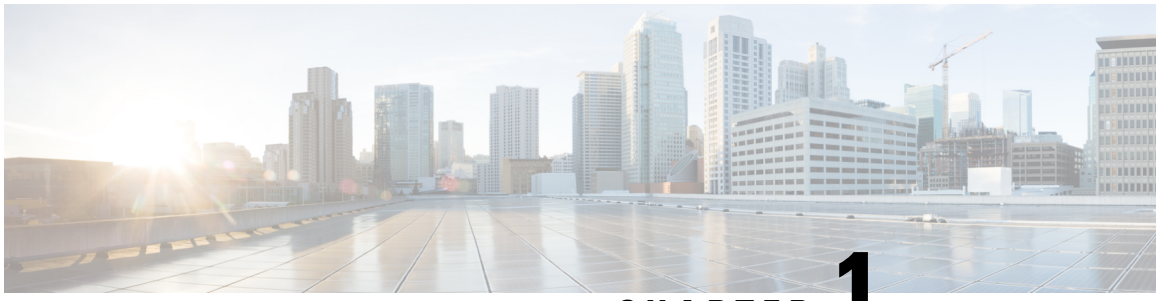
Crosswork Workflow Manager Solutions 2.1 Fleet Upgrade User Guide

First Published: 2026-01-30

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Get Started With Fleet Upgrade

This document covers the following topics:

About Fleet Upgrade

Cisco Crosswork Workflow Manager (CWM) Solutions is a collection of pre-built use cases that offers customers a convenient and efficient way to manage, configure and upgrade their devices. It provides out-the-box use cases that are easy to deploy and ready to use, allowing users to quickly onboard their devices for management.

CWM Solutions Fleet Upgrade lets users manage, distribute, and commit software images and image upgrades ato multiple devices at the same time, including to third-party devices.

Fleet Upgrade is automated, customizable, extensible, provides strong error checking, and supports devices from Cisco and other vendors.

To get started using Fleet Upgrade, see the next topic, Onboard devices, on page 2.

Pre-requisites

This version of Crosswork Workflow Manager Solutions (CWM-S) Fleet Upgrade is part of the Cisco Crosswork Network Controller Advantage tier. You must install the Advantage tier package as a CAPP (Crosswork APPlication) on an SVM (single virtual machine) deployment of Cisco Crosswork Network Controller.

Refer to Cisco Crosswork Network Controller 7.2 Installation Guide for instructions on cluster deployment and installation of the supporting products.

Onboard devices

Before you can test devices for compliance with software image standards, or upgrade them, the devices must be part of your Cisco Crosswork managed inventory.

The *Cisco Crosswork Network Controller 7.2 Administrator Guide* chapter Onboard Devices contains complete instructions on how to add devices to your managed inventory, using a wide variety of methods. Two of the mostly commonly used are:

- Adding devices one by one, using the GUI. For help with this method, see the topic Add Devices Through the User Interface.
- Adding devices in bulk by importing device information from a CSV template file. For help with this method, see the topic, Add Devices by Importing from CSV File

Once you have populated your managed device database, it is also a good idea to export it as a CSV file backup. For help with this task, see the topic Export Device Information to a CSV File.

Populate the image repository

Before you use Fleet Upgrade to standardize, test conformance, and upgrade the images installed on your network devices, you must first populate the Fleet Upgrade image repository with the images you need. You can then use these images set up the software image policies that establish your standards for image compliance.

Crosswork Workflow Manager Solutions Fleet Upgrade provides a local software image repository that you can use to set up policies that establish your software-image standards. You can then use the same repository to test whether your devices are in conformance with those standards, and deploy software images and upgrades to your managed devices. You can browse, choose and automatically download SMUs to the local repository directly from Cisco.com, using your Cisco customer login. You can also upload software images to the repository.

The topics in this section explain how to work with images in the repository:

Load SMUs from the Cisco catalog

Follow these steps to populate the image repository with images directly from the Cisco.com repository.

Procedure

Step 1 From the main menu, choose **CWM Solutions** > **Image Repository**. The Fleet Upgrade window's Image repository tab displays the list of ISOs and SMUs loaded to the local image repository.

Step 2 Click the **Cisco.com** tab. The window's **Image repository** section now displays the catalog of packages available from the Cisco.com software image download site.

Tip
Cisco releases many new SMUs each quarter. Use **Filters** to limit the display to the images of interest to you, as explained in Find images, on page 6. If you don't see the images you want, or the timestamps shown under **Synced** are more than

three months old, follow the steps in Update the Fleet Upgrade catalog, on page 8. You may also want to Inspect Cisco image details, on page 8 before downloading.

Step 3 Choose one or more of the images you want to download by clicking the checkboxes shown in the far left column in the same row as the **Image name**.

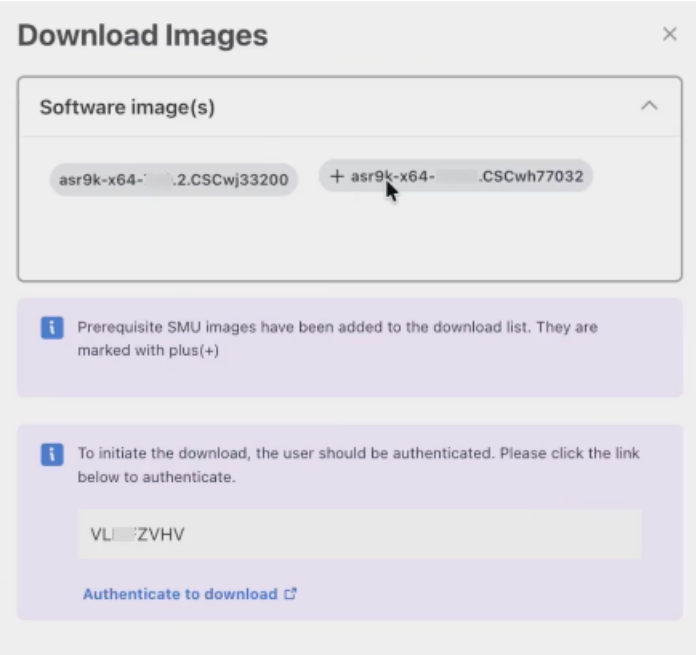
A green circle with a check mark shown next to the image's name under the **In local** column indicates that the image is already in the local repository.

Step 4 Choose **Download to local**.

Crosswork displays a **Download Images** popup window, listing the **Software Image(s)** you chose to download.

If any image you chose has dependent SMU images, they will be listed along with the main image. Each dependent image will be marked with a plus (+) sign. The popup will also display a user authentication code.

Figure 1: Download images



Step 5 Click the popup's **Authenticate to download** link to display a separate browser window. Then click **Next** to log in to Cisco.com with the authentication code and initiate the download(s).

The **Download Images** window remains displayed until you click **X** to exit.

Step 6 To check on download progress:

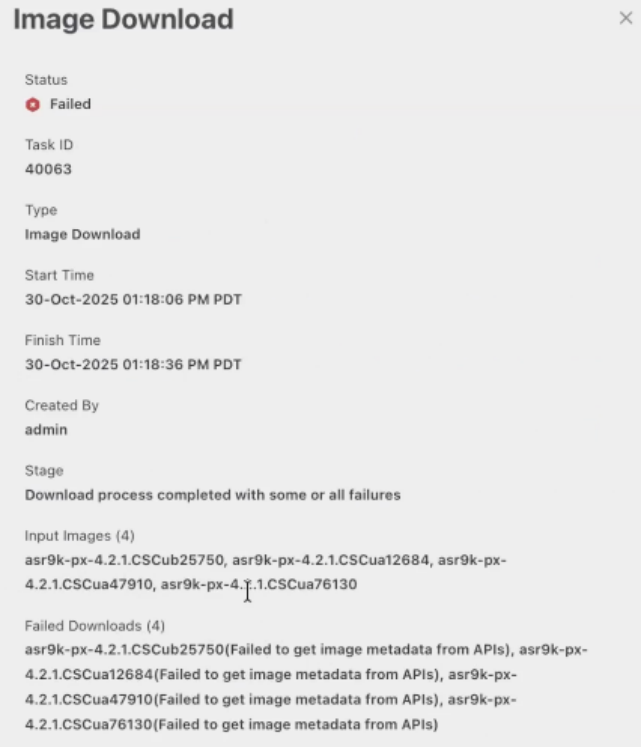
a) From the main menu, choose **Workflow Automation** > **CWM Solutions Systems Tasks**. Crosswork displays the list of running and completed systems tasks.

b) Look for an **Image Download** task you've recently initiated near the top of the list (or use the **Search** field to limit the display to this task type).

c) For details, click on the task's link in the **Type** column to display an **Image Download** popup with information on the task and its progress.

When the download task is complete, the popup will list causes for any downloads that failed.

Figure 2: Image download popup



Upload ISO images from a storage resource

Follow these steps to upload Cisco or third-party network ISO software images you have previously downloaded to a storage resource.

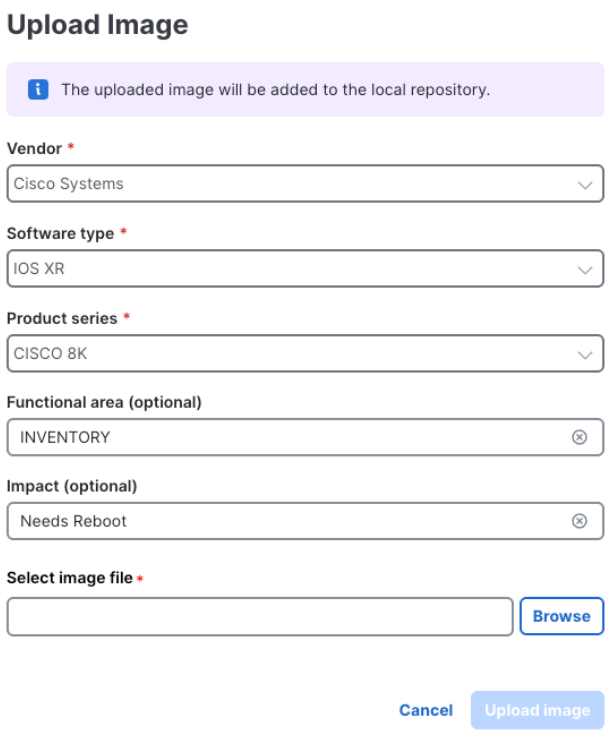
Procedure

Step 1 From the main menu, choose **CWM Solutions** > **Fleet Upgrade** > **Image repository**.

The **Fleet Upgrade** window's **Image repository** tab displays the list of images loaded to the local image repository.

Step 2 Click **Upload image** to display the **Upload Image** window.

Figure 3: Upload image to local repository



Step 3 Complete the fields on the **Upload Image** window as shown in the following table (the name of the image file, as well as values for the **Vendor**, **Software type**, and **Product series** fields are all required):

In this field...	Enter or choose:
Vendor *	**`Cisco`** or **`Juniper`**.
Software Type *	If **`Vendor`** is Cisco, **`IOS XR`** or **`IOS XE`**. If **`Vendor`** is **`Juniper`**, **`MX 960`**.
Product Series *	A supported Product Series for the chosen **`Vendor`** and **`Software Type`** (for example, **`CAT2000`**for **`Cisco`** and **`IOS XE`**).
Functional area (optional)	A description of the OS functional area affected by the upgrade (for example: **`ACL`** or **`Infrastructure`**).
Impact (optional)	A description of the operational impact of the upgrade installation (for example: **`Requires reboot`** or **`Hitless`**)
Select image file *	Enter the path and filename of, or click **Browse** to choose, the software image file to be uploaded.

Step 4 Once you have specified the image file, click **Upload image** to begin uploading the image to the repository.

Find images

Follow these steps to find an image downloaded to the local repository or in the Cisco.com catalog.

If you're looking for an image and can't find it in your local repository or in the Cisco.com catalog, synchronize the Fleet Upgrade catalog with the Cisco.com catalog and then search again. See Update the Fleet Upgrade catalog, on page 8.

Procedure

Step 1 From the main menu, choose **CWM Solutions** > **Fleet Upgrade** > **Image repository**.

Crosswork displays the list of images downloaded to the local repository, as shown below. If the image you want is not already loaded in the local repository, go to the next step.

Step 2 Click the **Cisco.com** tab to display the catalog of all SMUs available from the Cisco.com software image download site, as shown below.

Step 3 Once you are viewing the image catalog you want, use any of the following quick methods to find the image you want:

- Scroll the **Image repository** table until you see the name of the image you want to find.
- Begin entering characters in the **Search** field to narrow the table listing to only those images with names that match your search string.
- Click on any of the table column headings, such as **Image Name**, **Vendor**, **Software type**, **Product series**, **Image version**, and so on, to sort the table listing by the values in that column.

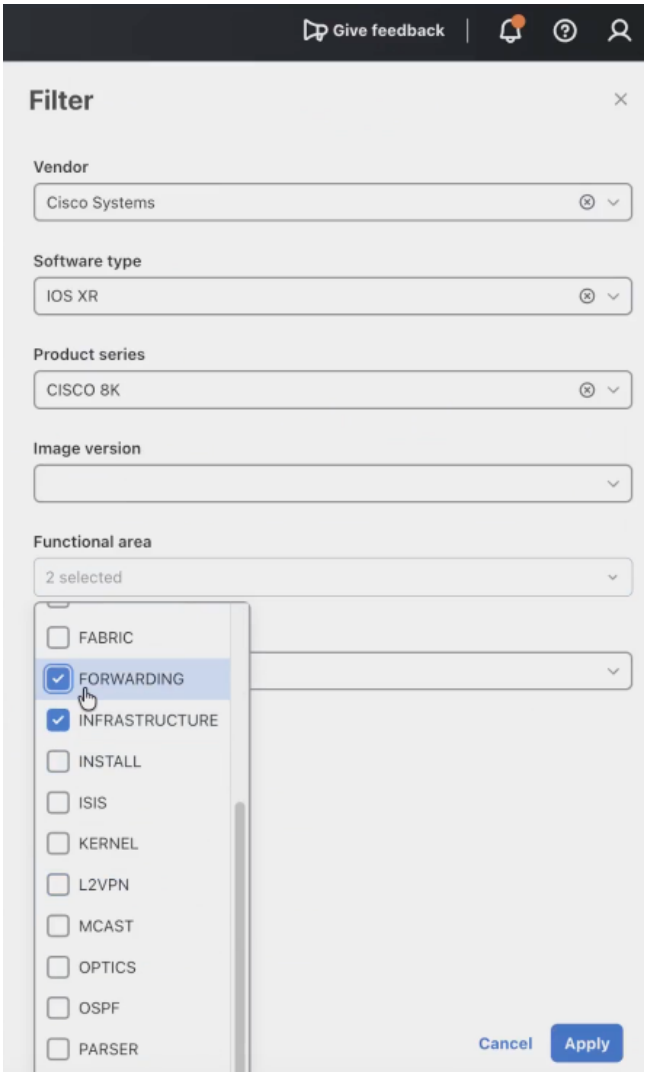
Step 4 Enter or select values in one or more of the filter fields (**Product series**, **Optimal**, and so on) at the top of the **Image repository** table. The filters you set will narrow the table listing to just those images that match the values you set.

Depending on which of the two **Image repository** tabs you are viewing and the **Filters** visible on your screen, you can filter on:

- the image **Vendor**
- the image operating system **Software type**
- the device **Product series** for which the image is intended
- the **Image version**
- whether the image is **Optimal** for the device or not
- the network **Functional area** the image affects
- the **Impact** the image will have on the device when applied
- the date and time the local copy of the image was **Last Updated**
- the date and time the Cisco.com image was last **Synced** with your local copy.

Step 5 If you want to use all of the filter fields at once, click on the **Filters** icon to display all the Filter fields in a **Filter** popup list at the right side of the table, as shown in the figure below.

Figure 4: Filter popup



When you have chosen all the filter values you want, click **Apply** to narrow the table listing to only those images with matching values. Click **Cancel** or the **X** icon. to exit the popup but retain the filters you set.

Click **Reset all** on the **Image Repository** window to clear the filters you set.

Step 6 If there is more than one page of listings: Use the **Rows per page** and page number controls at the bottom of the table to scroll to the page containing the image you want.

You can also click the **Table settings** icon (in the table heading row at far right) to change the table display density and the number of table columns shown.

Inspect Cisco image details

In addition to the information available to you in the **Image Repository** table view, you can click on the name of any image to see detailed metadata for the image, including a description, associated pre-requisites, lists of the packages included in it, related issue reports, the packages it supersedes, and much more.

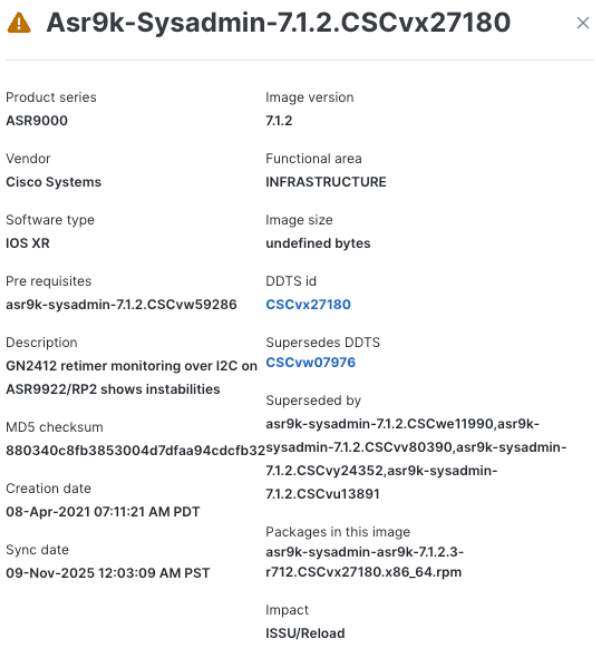
Procedure

Step 1 From the main menu, choose **CWM Solutions** > **Fleet Upgrade** > **Image repository**.

Step 2 Optional: If you want to view metadata for images in the Cisco.com repository, click the **Cisco.com** tab to display the Cisco.com image catalog.

Step 3 Under the **Name** column, click the name of the image whose details you want to see. Crosswork displays a popup details window like the one shown below. The popup title matches the name of the image.

Figure 5: Image details



Step 4 Some packages will contain links to Cisco Distributed Defect Tracking System (DDTS) software bugs and enhancement requests addresssed in a particular release. When links these links are included: Click on the **DDTS id** and **Supersedes DDTS** links to view web pages documenting these software issues.

Step 5 When you are finished, click the **X** icon to close the popup.

Update the Fleet Upgrade catalog

Cisco releases SMUs and related packages frequently. The catalog provided with Fleet Upgrade is a copy of the Cisco.com catalog and it is not updated automatically. It is a good idea to ensure that the Fleet Upgrade

copy of the catalog is in sync with Cisco.com, especially if you're having trouble finding an image that you want to download to the local repository, or you are creating image policies that include SMUs you have not yet downloaded.

Verify the results of the synchronization before continuing.

Procedure

Step 1 From the main menu, choose **CWM Solutions** > **Fleet Upgrade** > **Image repository**.

Step 2 Click the **Cisco.com** tab to display the Fleet Upgrade copy of the Cisco.com image catalog.

Step 3 Click **Sync catalogs**. Crosswork displays a confirmation warning.

Step 4 Click **Sync catalogs** again. Crosswork displays a message indicating that it has started the synchronization operation.

Step 5 To verify the results:

a) From the main menu, choose **Alerts** > **Alarms & Events** to display the **Alarms and Events** page.

b) Set the page to display **Events**. Look for events in the **System** category, with an **Information** severity level, that include the text `CCO sync`.

Create image policies

Software image policies are a critical part of the Fleet Upgrade workflow. Whenever you create a software image policy, you choose one or more software image versions and make them part of the standard set of images to be installed on your devices.

As different types of devices run different types of software images, you'll need to establish image policies for each type of device. Whenever you run a Fleet Upgrade conformance report against a particular type of device, you will also need to pick the appropriate image policy for that device type. The Fleet Upgrade workflow will then check the software actually installed on those devices against the standard image established in the policy. If the installed and standard image versions don't match, then the device is non-conformant.

Fleet Upgrade will rate as conformant only those devices that have installed on them *all* of the target images and versions in the image policy at the time you run the conformance report. If you run a conformance report against a device that does not have one or more of the policy's images or versions installed, the report will rate that device as non-conformant.

Note With this release of Fleet Upgrade, you do not need to load into the local repository all the SMUs for a particular software version beforehand in order to add them to a software image policy. As long as your local Fleet Upgrade SMU catalog is in sync with the Cisco.com catalog, you can select both local and non-local SMUs for inclusion in an image policy. See Update the Fleet Upgrade catalog, on page 8.

Procedure

Step 1 From the main menu, choose **CWM Solutions** > **Fleet Upgrade** > **Software conformance** > **Image policies**.

Step 2 Click **+ Add image policy** to display the **New image policy** window.

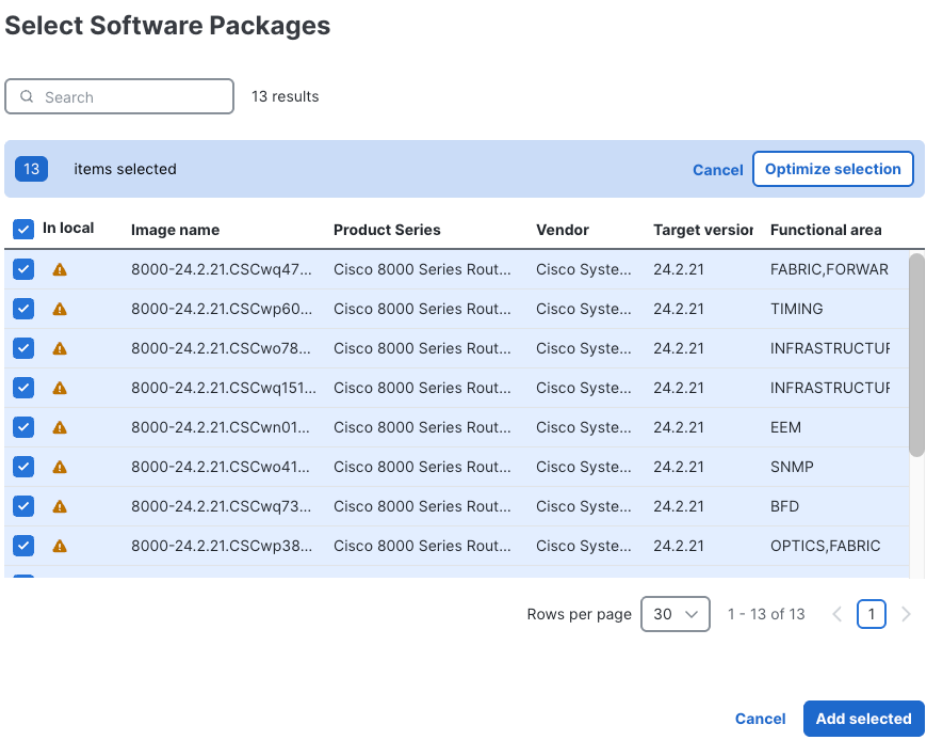
Step 3 Complete the first five fields in the **New image policy** window as shown in the following table:

In this field...	Enter or choose...
Policy name	A unique name for the image policy, such as **`ASR 1K Basic SMU Mix`**.
Description	An optional description of the policy's purpose, such as **`Standard minimum SMU level for all Cisco ASR 1000 routers`**.
Vendor *	The name of the software vendor, such **`Cisco Systems`**.
Product series *	The network device product series, such as the **`Cisco ASR1000`**.
Target version *	The target version of the product series, such as **`17.09.04a`** for the **`Cisco ASR1000`**. Supported target versions are pre-selected for you based on the Vendor and Product series you choose. Note that you cannot change the **Vendor** and **Product series** value once you have chosen a **Target version**.

Step 4 In the **Software packages** field, click the **+ Add** button. The **Select Software Packages** window lists all the software images that can be installed on the network device product series you specified (including images not locally downloaded).

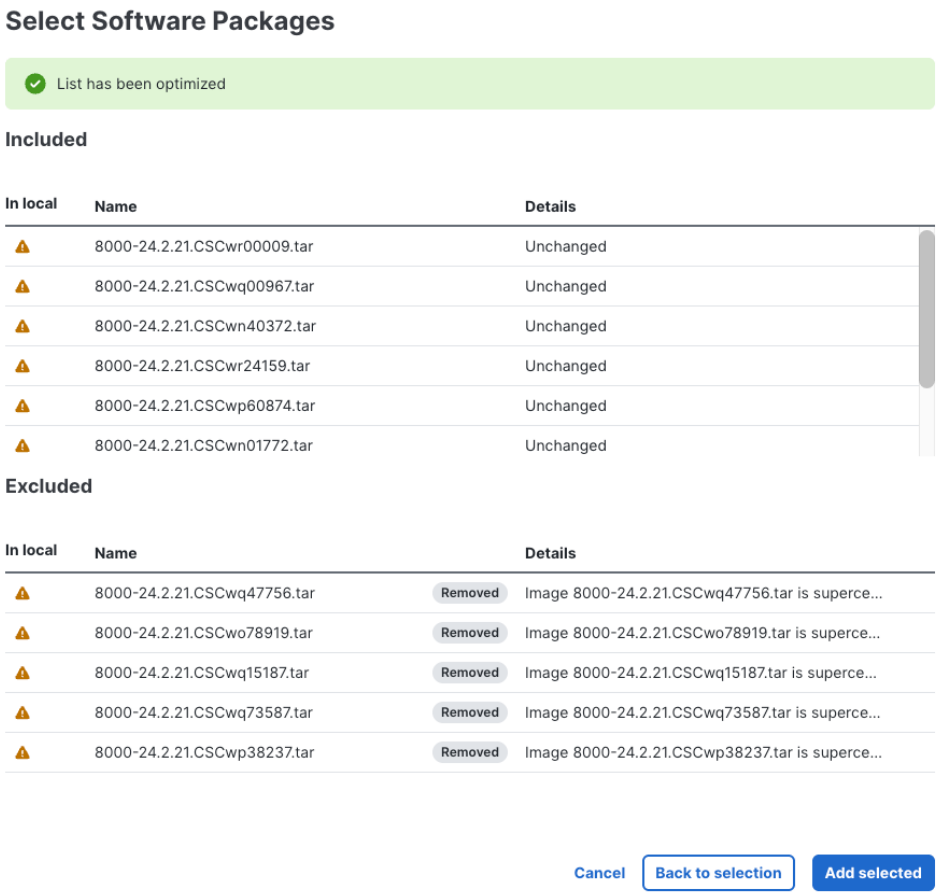
Step 5 Click the check box in the same row as the **Image name** of each software image you want to make part of this image policy.

Figure 6: Select Software Packages



Step 6 **Optional**: If you have selected multiple packages and want to ensure that only those that are actually required are included, click **Optimize selection**. Crosswork displays an optimized version of your list, with essential packages in an **Included** section at the top and non-essential packages in an **Excluded** section at the bottom.

Figure 7: Select Software Packages - Optimized selection



If you click **Add selected** now, only the **Included** packages will be part of the policy. To revise your selections further, click **Cancel** or **Back to selection**.

Step 7 When you are finished selecting packages, click **Add selected**. Crosswork displays your policy settings and the list of packages you selected.

You can revise the **Policy name**, **Description**, and **Target version**, or click **+ Add** to change your package selections.

Step 8 When you are finished, click **Save changes** to create and save the new policy. Crosswork displays the **Image policies** window with your new policy listed in the table.

What to do next

Follow the steps in Run a policy conformance report, on page 12.

Run a policy conformance report

Use the policy conformance report to determine when you need to perform a Fleet Upgrade on one or more of your network devices.

You can create Fleet Upgrade conformance reports to check software image conformance for any device type and any combination of software images and versions. The core of the report is the software image policy you choose. The software image policy specifies the standard software images your devices should have installed on them. In addition, you can choose to run Fleet Upgrade conformance reports against devices on demand, at a future date or time you choose, or at regular recurring intervals. Each time the report runs, it will compare the software image installed on the devices with the software images specified in the image policy. The report will identify as "conformant" every device with all the policy's images installed. The report will flag as "non-conformant" any devices missing one or more of the policy images.

Tip You may find that the image policy that forms the basis of the conformance report you ran is out of date or otherwise incorrect. If that's the case, you can easily edit the policy and then run the report again.

To edit an existing image policy, select **CWM Solutions** > **Fleet Upgrade** > **Software conformance** > **Image policies** to display the list of image policies. Scroll or use **Search** to find the policy you want, then click the **More (…)** menu at the far right in the same row as the report you want and select **Edit report**.

Before you begin

Ensure you have created one or more software image policies, as explained in Create image policies, on page 9.

Procedure

Step 1 From the main menu, choose **CWM Solutions** > **Fleet Upgrade** > **Software conformance** > **Conformance reports**. The **Conformance reports** tab displays the status of all completed software conformance reports.

Step 2 Click **+ New report**.

Step 3 Complete the first five fields in the **New image policy** window as shown in the table:

In this field...	Enter or select...
Report name	A unique name for the conformance report, such as **`ASR1KStandard`**.
Select image policy	An optional description of the policy's purpose, such as **`Cisco ASR 1000 edge router SMU status`**.
Current version	The device software version number, such as **`24.2.2`**.

In this field...	Enter or select...
Run schedule	One of the following: • **Run now**. • **Schedule for specific data and time**. If you select this option, you must also specify a **Time** and **Date**. • **Run recurring report**. If you select this option, you must also specify an **Interval** between runs, or the **Days of the week** or **Days of the month** you want the recurring report to run on.

Step 4 When you are finished, click **Create Report** to save the new report. If you selected **Run now**, you will also run the new report.

Clicking **Create Report** will return you to the **Conformance reports** tab, where you can review the status of any report you have already run.

What to do next

If you're still viewing the results of a report and you see non-conforming devices, consider running a Fleet Upgrade using the steps in Run a Fleet Upgrade job, on page 14.

If your conformance report failed, investigate by following the steps in Monitor conformance report results, on page 13.

Monitor conformance report results

Use the **Conformance reports** tab to monitor the results of a conformance report, including any failures that occur. The status details for failures will help you diagnose the cause and correct it.

Procedure

Step 1 From the main menu, choose **CWM Solutions** > **Fleet Upgrade** > **Software conformance** > **Conformance reports**.

Step 2 Click the **Latest status** column header to sort the column alphabetically. Reports with "Conformant" and "Failed" results will be sorted and displayed.

Step 3 **For any report that failed**: Click the **Report** name. Crosswork displays a detail screen like the one shown below, giving the reason for the report failure. In this example, no existing devices were specified, so there was nothing against which to compare the software image policy. You can easily correct this by ensuring that the next run includes devices.

Tip
For any software conformance report whose details you're viewing:

- Click on the date field to see details for other runs of the same report.
- Click **Edit report** to change the report settings and re-run or re-schedule it.
- Click **Export to CSV** to save the report as a CSV file in your default downloads directory.

- Click **Run instantly** to re-run the report immediately with the same settings as before.

Step 4 **For any report showing non-conformant devices**: Click the **Report** name. Crosswork displays a detail screen like the one shown below, listing the non-conformant devices. If needed, click the **Device** name to see details for each non-conforming device. In this example, the first of the three devices was missing both of the required software packages.

Run a Fleet Upgrade job

Fleet Upgrade uses Methods Of Procedure (MOPs) to perform automated device upgrades. The term "MOP" as used in Fleet Upgrade refers to a set of pre-programmed actions that are performed in sequenced phases. Each Action in the MOP is selected and (where needed) customized to deliver a complete, successful upgrade for the combination of software image and device for which it is intended. Fleet Upgrade provides default MOPs for the devices and software it supports, as well as facilities for creating custom versions of the default MOPs, and entirely new MOPs with mixtures of default and new Actions. At runtime, you have the opportunity to select which MOP your Fleet Upgrade job will use, as well as customizing other variables (such as the job name and the execution schedule). For more on these topics, see Use the default MOPs, on page 21.

Before you begin

The easiest way to run a Fleet Upgrade is, first, to run a conformance report, as explained in Run a policy conformance report, on page 12, and then select the non-conforming device and click **Start Fleet Upgrade**. Running the conformance report first not only ensures that the Fleet Upgrade is really needed, it also lets you launch the upgrade automatically.

The steps below assume that you will want to launch a Fleet Upgrade from the **Software conformance** > **Conformance report** window. But you can also launch an upgrade by clicking the **Start Fleet Upgrade** button on any of the other **Fleet Upgrade** windows where it appears: **Devices**, **Image repository** > **Local repository**, **Image repository** > **Cisco.com**, **Software conformance** > **Image policies**, **MOPs**, and **Jobs**,

Procedure

Step 1 From the main menu, choose **CWM Solutions** > **Fleet Upgrade** > **Software conformance** > **Conformance reports**. The list should show a **Report** with one or more devices with a **Latest status** that is **Not Conformant**.

Step 2 Click the selection checkbox shown next to the name of the **Report**. Click **Start Fleet Upgrade**. The **New Software Update** window displays a list of all the devices that were checked for conformance. The non-conformant devices are already selected for you.

Step 3 For each additional device you want Fleet Upgrade to update, click the check box shown next to the device **Host name**. Or click the check box shown next to the **Host name** column title to select all of them.

You can select a maximum of 50 devices to be upgraded in the same Fleet Upgrade job.

Step 4 Click **Next** to display the **Select software image** window. If the software image policy you used to create the conformance report specified a target version and software packages, the list of software packages to be installed on the devices will be pre-selected for you.

Step 5 If the image policy did not specify packages, or you want to install more packages, click **+Add**, then click the check box shown next to each package's **Image name**. Then click **Select** to display the list of all packages to be installed.

Step 6 Click **Next** and then click the **Select MOP** drop down list to select the MOP you want to use to install the chosen software packages on the selected devices.

The drop down list will always display one or more MOPs pre-selected for the type of device series you are trying to upgrade. Unless you have a special purpose in mind, use the pre-defined MOPs supplied with Fleet Upgrade, such as the **Default XR Upgrade** MOP as shown in the figure.

Step 7 Click **Next** and fill the fields in the **Execution settings** window.

In this field...	Enter or select...
Job name	A unique name for the job, such as **`ASR1KStandard`**.
Job tags	An optional, comma-separated list of search tags to help you find the job in the job listing, **`ASR1000, ASRUpdates`**.
Parallel upgrades	Specify the number of device upgrades to be executed at the same time, in parallel. Defaults to 1. For help with setting this and the **Acceptable failures** value, see Use parallel upgrades with acceptable failures, on page 19.
Acceptable failures	Specify the number of installation failures to be allowed before further upgrades are canceled. Defaults to 1.
Execution time	Specify one of the following: • **Run now**. Fleet Upgrade will begin executing the upgrade as soon as you click **Submit**. • **Schedule for specific data and time**. If you select this option, you must also specify a **Time** and **Date**.

Step 8 Click **Next** to display the **Summary** window.

Step 9 When you are finished, make sure the confirmation checkbox is selected. Then click **Submit** to save the new update job and either schedule or (if you selected **Run now**) run it.

What to do next

Follow the steps in Monitor Fleet Upgrade job results, on page 15.

Monitor Fleet Upgrade job results

Use the Fleet Upgrade **Jobs** page to monitor the results of a Fleet Upgrade job run, including any failures that occur. The status details for failures will help you diagnose their cause.

Procedure

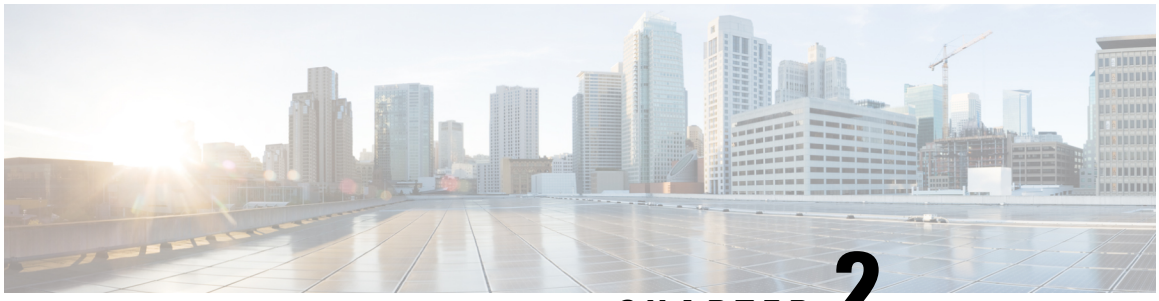
Step 1 Choose **CWM Solutions** > **Fleet Upgrade**. Click **Automations** and select **CWM solutions jobs** to display the list of upgrade jobs and their status.

Step 2 Click the **Status** column header to sort the column alphabetically.

Step 3 Click the **Job name** for a job that failed. A **Job Summary** page is displayed. Under **Device results**, the page lists the **Host name** of the device where the update failed and the **Last finished stage** where the failure occurred.

Step 4 Click the **Host name** to display a pop up screen with tabs representing the stages of the upgrade, and for each stage, the actions performed during that stage.

Step 5 Click the tab for the stage where the upgrade failed and expand the action where the failure occurred to see more details.



CHAPTER 2

Customize Fleet Upgrade

This document covers the following topics:

Build Cisco GISOs

Follow these steps to build a Golden ISO (also known as GISO, golden image or master image) from a IOS XR or XE bootable base ISO, one or more system patches (SMUs), and other optional packages and configuration files.

GISOs are a popular, efficient way to establish a standard baseline system configuration for each category of device you deploy. They help ensure that all new deployments and upgrades include the same base capabilities and mix of fixes. They reduce human error, ensure consistency, and lead to optimized performance and reduced image size.

To build a GISO, you must select one installable Cisco ISO software image to serve as the base. You can then add SMUs and other packages as you choose. The ISO can be any bootable ISO (including mini and K9 ISOs). Both the ISO and the other packages must already be loaded into the local repository.

Before you begin

Image availability: Ensure all required images are present in the local image repository before starting the GISO build to prevent interruptions.

EXR optional packages: For EXR platform Golden ISOs, include optional packages specific to the product series and software version. Collect the necessary RPM files and bundle them into a TAR archive for upload, following the required naming convention.

TAR naming convention: The tar filename format typically follows the pattern: platform-image_type-release.tar. For example, ASR9K-x64-iosxr-25.2.2.tar, NCS540-iosxr-25.2.2.tar, NCS540l-aarch64-iosxr-optional-rpms-25.4.1.tar.

Resource usage during Golden ISO creation: Golden ISO creation may briefly use additional system resources. As a result, some uploads or downloads could be temporarily limited. Normal operations will resume automatically once the process completes.

Procedure

Step 1 From the main menu, choose **CWM Solutions** > **Fleet Upgrade** > **Image repository**.

Crosswork displays the list of images downloaded to the local repository.

Step 2 Click **Build GISO**. Crosswork displays the **Generate GISO** window, with a **Process Overview** listing the steps in the GISO generation workflow.

Step 3 Click **Next** to display the **Select base ISO** window. Crosswork lists all the ISO images in the local repository. Click the selection checkbox next to the base ISO you want to use.

Step 4 Click **Next** to display the **SMU selection** window, listing all the SMU packages in the local repository. Click the selection checkbox next to the **Name** of each SMU or other package you want to include in the GISO.

Note that you will not be able to select any packages that are not already in your local repository. You will need to download these packages first to include them in a GISO.

Step 5 Click **Next** to display the **Refined SMU List** window.

The **Included List** in the upper part of the window lists all the SMUs and other packages you selected that are in the local repository and will be included in the GISO.

Fleet Upgrade will also include any packages required by your selections that are also in your local repository. Fleet Upgrade adds these packages to the **Included List** automatically, and indicates this with the **Added** flag, along with **Details** explaining why they were added.

The refinement process performs the following:

- Adds any dependent SMUs required by your selections that were not initially selected.
- Removes SMUs that are superseded by other selected SMUs.
- Lists whether required images are present in the local image repository. If a required image or component is missing from the local repository, Golden ISO (GISO) creation will be blocked until you upload or download the missing image.

Obsolete or otherwise inappropriate packages that you selected will be shown in the **Excluded List**. Fleet Upgrade excludes these automatically, indicating this with the **Removed** flag, and explaining the reason for their exclusion in the **Details** column. These packages will not be included in the GISO.

Step 6 Click **Next** to display the **Summary** window.

Review your selections. If you are satisfied, click **Generate GISO** to begin building your GISO. Golden ISO creation typically takes 20–180 minutes, depending on the number and size of SMUs and optional packages selected.

After submission, you will be redirected to the **CWMS Systems Task** page, where you can monitor the status of your GISO build task in real time. Your recently initiated GISO build should appear among the **Running** tasks in the task list. Alternatively, select **Workflow Automation** > **CWMS Systems Tasks** to check on the progress of the GISO build. The task details page shows the current status, additional details, and any errors encountered during the build process.

Upon successful completion, the newly created Golden ISO will be added to the local images list and will be available for Fleet Upgrade.

Use parallel upgrades with acceptable failures

Fleet Upgrade provides the **Parallel upgrades** and **Acceptable failures** fields to help you both speed up and control long upgrade runs with many devices.

As explained in Run a Fleet Upgrade job, on page 14, whenever you create a Fleet Upgrade job, you can select up to 50 devices to be upgraded during that job. Depending on the number and size of each device upgrade, this can result in jobs lasting hours. This would be worse if you had to upgrade each device one at a time, in series. It would be still worse if you couldn't cancel the run if you started experiencing upgrade failures.

To help with these issues, you can use the **Parallel upgrades** field to specify how many upgrades you want performed at the same time, in parallel. If you enter a **Parallel upgrades** value equal to the total number of devices to be upgraded (up to the maximum of **`50`**), all the upgrades will take place at the same time. If you leave **Parallel upgrades** set to the default value of **`1`**, Fleet Upgrade performs each of them one at a time.

Most users specify a lower **Parallel upgrades** value, such as **`5`** or **`10`**. Doing so helps conserve processing resources and ensures that only a few of the network devices in a 50-device job set will be offline at one time.

With a lower **Parallel upgrades** value, Fleet Upgrade performs the upgrades in batches. For a 50-device upgrade group with a **Parallel upgrades** value of **`5`**, this means 10 batches of five upgrades each. In this case, Fleet Upgrade performs all five of the upgrades in batch #1 at the same time, in parallel, and doesn't initiate any of the upgrades in batch #2 until all of the upgrades in batch #1 are finished.

How can you cancel a job that's failing too often? Fleet Upgrade will automatically cancel the remaining upgrades in a job depending on the number of **Acceptable failures** you set. The value you specify in this field acts as a failure "budget" that, when exceeded, triggers automatic cancellation of all of the remaining upgrades in the run. If you want to avoid automatic cancellation entirely, specify an **Acceptable failures** value equal to the total number of devices to be upgraded (up to the maximum of **`50`**). Set it to the default value of **`1`** if you want the system to cancel remaining upgrades after the very first failure.

Bear in mind that a batch will run to completion once started. The error budget defined in **Acceptable failures** will block additional batches from starting if it has been exceeded. Sometimes, this means the total number of actual failures will exceed the failure budget, and it will take longer for cancellation to kick in than you might expect.

For example: Let's assume that our job set is 50 devices. Our **Parallel upgrades** setting is 5 and our **Acceptable failures** setting is 5. That means we have 10 batches of 5 devices for Fleet Upgrade to perform. Let's further suppose that, during execution of batch #1, we encounter 4 failures. The 5-failures budget is not yet exceeded, so Fleet Upgrade will begin to execute all the upgrades in batch #2 in parallel. We then encounter 4 more failures in batch #2. The 5-failure budget is now exceeded, so Fleet Upgrade will automatically cancel execution of batch #3 and the remaining 7 other batches. However, we've actually encountered 8 failures, not 5. Similarly, we might encounter only 1 failure each in batches #1, #2, #3, and #4, then encounter 1 more failure in batch #5. We now have a total of 5 failures, but this does not *exceed* the failure budget, only *equals* it. So Fleet Upgrade then goes on to the next batch. Then, in batch #6, every upgrade fails, exceeding the failure budget and triggering cancellation of the run. In this case, we've actually encountered 10 failures, twice the number we specified. Also, cancellation wasn't triggered until batch #7 and device #35, some 70 percent of the way through the entire run.

Download software upgrades using a proxy server

You can download Cisco SMUs to your local image repository using a proxy server, but you must configure the proxy first, using the following steps.

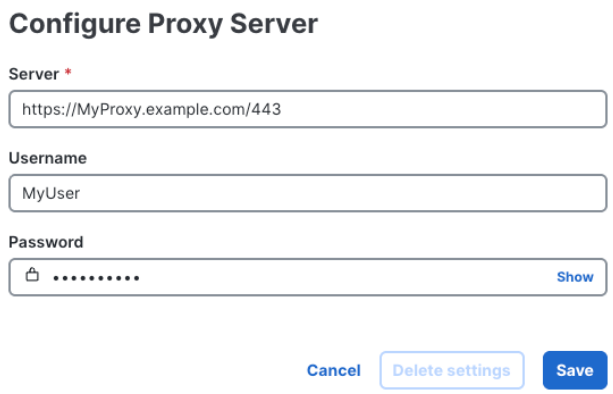
Procedure

Step 1 From the main menu, choose **CWM Solutions** > **Fleet Upgrade** > **Image repository**.

Step 2 With the contents of the **Image repository** displayed, click the **Cisco.com** tab to display the Cisco.com image catalog.

Step 3 Click **Configure proxy server** tab to display a popup like the one shown below.

Figure 8: Configure proxy server



Step 4 Complete the proxy server fields as needed. When you are finished, click **Save**.

You must enter the **Server** URL or IP address and port number. You must also enter a valid **Username** and **Password** if the proxy server requires a login.

Troubleshoot Fleet Upgrade failures

The following table summarizes common Fleet Upgrade issues and their remedies.

Table 1: Common Fleet Upgrade Issues and Remedies

Issue	Description	Remedy
Upgrade fails; unable to transition state	Upgrade fails due to inability to transition state during image distribution	Increase timeouts to at least 3600 seconds for Action, Event, State, and Workflow. System Activity timeout should be at least 10 seconds.

Issue	Description	Remedy
FPD causes activation failure	The failure message will include a recommendation that you "Please reconfigure your settings and create a new job." Upgrade fails during "Activate" stage, with the following message: "Performing FPDs upgrade on the device. FPDs upgrade success except for the following FPDs: PO-PrimMCU, PO-PrimMCU". This occurs on VXR devices.	Add the following to the `Activate` Action configuration input: `"fpd": "false","isISSUUpgrade": "false" }`
Fleet Upgrade GUI drop downs are not working	The Vendor, Product series and other GUI drop down selection lists don't appear when clicked on.	The issue occurs when NSO packages are not updated. Please install the correct packages when installing Fleet Upgrade.
Software Image Policy has no Vendor or Device drop down	The Vendor and Product series drop down selection lists don't appear when clicked on.	Check that at least one software image has been downloaded to the local image repository. Fleet Upgrade is designed to display Vendor and Product series selections only when software images are available in the local repository.
Upgrade fails due to failure to find FTP services	Upgrade fails with a message indicating that a `Distribute` action failed due to the FTP server not being found.	From the main menu, select **Administration** > **File servers** and ensure that **Enable FTP** and **Enable SFTP server upload** are both checked. Also ensure that your organization's FTP and SFTP servers are active on TCP Ports 30621 and 30622, respectively.

Use the default MOPs

Fleet Upgrade comes installed with default (or "pre-built") MOPs. These MOPs are provided by Cisco, cannot be modified directly (although they can be copied and the copies modified), and are intended for use in performing upgrades for specific supported vendors and device families:

- **Default Juniper Upgrade**: For upgrading Juniper MX960 series devices running JunOS
- **Default XE Upgrade**: For upgrading Cisco Systems ASR 900 series devices running Cisco IOS-XE
- **Default XR Upgrade**: For upgrading Cisco Systems 8000 series devices running Cisco IOS-XR

In most cases, you will want to select one of these default MOPs when a conformance report indicates that it is time to upgrade a suppported device in the series. They are usually your safest choice when upgrading devices from these manufacturers. Each of the default MOPs is customized for the supported vendor and

product series, and the customizations are extensive. Each MOP varies significantly in the number of action types it makes available, the selected actions it performs during an upgrade, and the stages it goes through as it performs these actions. For example:

- **Default Juniper Upgrade**: Offers 17 action types. The majority of these Actions are Juniper-specific. It performs 19 Actions during an upgrade: nine during the Pre check stage, three during the Distribute stage, one during the Activate stage, and six during the Post stage.
- **Default XE Upgrade**: Offers 15 Action Types. It performs 17 Actions during an upgrade: seven during the Pre check stage, two during the Distribute stage, one during the Activate stage, and seven during the Post stage.
- **Default XR Upgrade**: Offers 22 Action Types. It performs 25 Actions during an upgrade: 11 during the Pre check stage, three during the Distribute stage, three during the Activate stage, one during its unique Commit stage, and seven during the Post stage.

However, running a default MOP may not always be your best choice for an efficient, targeted upgrade. You may find it useful to view each default MOP as a comprehensive library of all the Fleet Upgrade Actions relevant to a particular vendor and product series, arranged as a useful workflow.

You don't have to stick with the default MOP. You can copy a default MOP, and then manipulate and customize the copy to suit your needs. For example, you may decide that a MOP step that checks existing disk space is not necessary when you are upgrading software on a set of devices that are all factory-fresh. Similarly, you may that find running sanity checks against devices that you know are up and running is a waste of time and don't belong in the MOP you want to run. For more information about creating custom MOPs, see the *Cisco Crosswork Network Controller Solutions 7.2 MOP User Guide*